Verfahren zur Identitätsprüfung

Publication number: DE19715644 (A1)
Publication date: 1998-10-22
Inventor(s): BOOKHAGEN JENS [DE]; DONNERHACKE LUTZ [DE]; STEGER HENRY [DE]; WENIGER KLAUS [DE]
Applicant(s): IKS GMBH INFORMATION KOMMUNIKA [DE]
Classification:
- international: ***G07C9/00; G07F7/10; H04L9/08; H04L9/32;*** **G07C9/00; G07F7/10; H04L9/08; H04L9/32;** (IPC1-7): G06K9/62; A61B5/117; G07C9/00; G07F7/08; H04L9/32
- European: G07C9/00C2D; G07F7/10D6K; G07F7/10E; H04L9/08; H04L9/32
Application number: DE19971015644 19970415
Priority number(s): DE19971015644 19970415

Also published as:
WO9847110 (A1)

Cited documents:
DE2341627 (C2)
US5615277 (A)
EP0731426 (A2)
WO9705578 (A1)

Abstract of **DE 19715644 (A1)**

The present invention relates to an identity verification procedure as a prerequisite to granting an access and/or use permission, whereby at least one data set based on biometrical signs enabling identification is built using a data entry and processing system. The invention also relates to facilities for implementing said method. In order to fulfil that task, the biometrical features are first captured in the form of reproductible feature data; a first data set is then generated from random data, which data set is stored on a data medium as a control data set; at least part of the feature data is related to at least part of the control data set and converted by a non-reversible computing operation into a second data set; and this second set is used as a criterion fo granting an access and/or use permission and/or as a cryptographical key setting.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 15 644 A 1**

(51) Int. Cl.[6]:
G 06 K 9/62
G 07 C 9/00
G 07 F 7/08
A 61 B 5/117
H 04 L 9/32

(21) Aktenzeichen: 197 15 644.4
(22) Anmeldetag: 15. 4. 97
(43) Offenlegungstag: 22. 10. 98

(71) Anmelder:
IKS GmbH Information-Kommunikation-Systeme, 07745 Jena, DE

(74) Vertreter:
Dr. Werner Geyer, Klaus Fehners & Partner, 07745 Jena

(72) Erfinder:
Bookhagen, Jens, 07751 Jenaprießnitz, DE; Donnerhacke, Lutz, 07747 Jena, DE; Steger, Henry, 07743 Jena, DE; Weniger, Klaus, 07646 Waldeck, DE

(56) Entgegenhaltungen:

DE	23 41 627 C2
US	56 15 277 A
EP	07 31 426 A2
WO	97 05 578 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Identitätsprüfung

(57) Die Erfindung bezieht sich auf ein Verfahren zur Identitätsprüfung als Voraussetzung für die Erteilung einer Zugangs- und/oder Ausübungsberechtigung, bei dem mit Hilfe eines Datenerfassungs- und Datenverarbeitungssystems mindestens ein Datensatz auf der Grundlage biometrischer Merkmale erzeugt wird und bei dem der Identitätsnachweis anhand der zugrundeliegenden biometrischen Merkmale erfolgt. Die Erfindung bezieht sich weiterhin auf Anordnungen zur Durchführung dieses Verfahrens.

Die Aufgabe der Erfindung wird dadurch gelöst, daß in einem ersten Verfahrensschritt charakteristische biometrische Merkmale in Form hinreichend reproduzierbarer Merkmaldaten erfaßt werden, daß in einem weiteren Verfahrensschritt ein erster Datensatz aus Zufallsdaten generiert und als Steuerdatensatz auf einem Datenträger abgelegt wird, daß mindestens ein Teil der Merkmaldaten mit mindestens einem Teil des Steuerdatensatzes verknüpft und durch eine nicht umkehrbare Rechenoperation in einen zweiten Datensatz transformiert wird und daß der zweite Datensatz als Kriterium für die Erteilung der Zugangs- und/oder die Ausübungsberechtigung und/oder als Kryptographieschlüssel verwendet wird.

DE 197 15 644 A 1

DE 197 15 644 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Identitätsprüfung als Voraussetzung für die Erteilung einer Zugangs- und/oder Ausübungsberechtigung, bei dem mit Hilfe eines Datenerfassungs- und Datenverarbeitungssystems mindestens ein Datensatz auf der Grundlage biometrischer Merkmale erzeugt wird und bei dem der Identitätsnachweis anhand der zugrundeliegenden biometrischen Merkmale erfolgt. Die Erfindung bezieht sich weiterhin auf Anordnungen zur Durchführung dieses Verfahrens.

Unter dem Gesichtspunkt aktueller Entwicklungstendenzen in der Gesellschaft besteht zunehmend das Bedürfnis, einen unberechtigten Zugang zu Sachen, eine unberechtigte Auslösung von Vorgängen und/oder eine unbefugte Ausübung von Handlungen auszuschließen. Im Zusammenhang damit sind verschiedenartige Verfahren und Anordnungen entwickelt worden, die eine Zugang- bzw. eine Ausübungserlaubnis erst nach erfolgreich vorgenommener Identitätsprüfung von Personen erteilen.

So ist in der Patentschrift DE 43 22 445 C1 ein Verfahren zum Codieren von Identifikationskarten mittels Fingerabdrücken beschrieben, bei dem mit Hilfe eines Sensors vom Inhaber der Identifikationskarte eine Mehrzahl von Fingerabdrücken abgenommen wird, von den abgenommenen Fingerabdrucken ein Abdruck als Schlüsselcode auf die Identifikationskarte aufgebracht wird und nach einem Verwirbelungsschlüssel mindestens einer der anderen Fingerabdrücke als Identifizierungscode ausgewählt und gespeichert wird. Der Schlüsselcode-Fingerabdruck kann beispielsweise in Form eines Hologrammes gespeichert werden.

Das hier vorgeschlagene Verfahren sieht vor, daß der Karteninhaber seine Identifikationskarte in eine Fingerabdruck-Vergleicheinrichtung einschiebt und eine Mehrzahl oder alle Finger beider Hände auf einen Fingerabdrucksensor legt. Es erfolgt ein Vergleich des auf der Karte gespeicherten Fingerabdruckes mit einem der natürlichen Fingerabdrücke, wonach bei positivem Vergleich mittels eines abgegebenen Ausgangssignales ein Zugang zu einem Speicher geöffnet wird, der den nach einem Verwürfelungssystem ausgewählten Fingerabdruck des Karteninhabers enthält. Dieser Speicher kann ein lokales Terminal am Einsatzort der Karte sein. Vorgeschlagen wird aber auch ein zentrales Terminal, das mit dem Fingerabdruck-Vergleichsgerät am Einsatzort verbunden ist. Mit dem geöffneten Zugang zum Speicher erfolgt ein Vergleich des gespeicherten Fingerabdruckes mit den übertragenen Fingerabdrücken und bei Übereinstimmung des gespeicherten Fingerabdruckes mit einem der übertragenen Fingerabdrücke eine Freigabe der Identifikationskarte.

Aufgrund der doppelten Codierung wird ein relativ hoher Sicherheitsstandard erreicht. Nachteilig dabei ist jedoch, daß bei einer Vielzahl von Benutzern, deren Zugangsberechtigung zu prüfen ist, eine hohe Kapazität zur Speicherung aller Fingerabdrücke erforderlich ist, und daß außerdem jeder Benutzer eine Identifikationskarte bei sich haben muß.

Eine anderweitige Verfahrensweise mit zugehöriger Anordnung ist in der DE 42 20 971 A1 beschrieben. Hier wird eine Fingerabdruck-Abtastvorrichtung zur Identitätsprüfung genutzt, bei der eine Bildeingabeeinrichtung mit einer Speichereinrichtung zum fotoelektronischen Speichern von Fingerabdrücken registrierter Personen gekoppelt ist. Eine Merkmalerkennungseinrichtung verarbeitet die Bilddaten und erzeugt ein Spektrenmuster. Eine Bestimmungseinrichtung identifiziert die eintretende Person als registrierte Person. Eine Ausgangssignaleinrichtung erzeugt ein Entriegelungssignal und sendet es an eine Türschließeinrichtung.

In der hier genutzten Merkmalerkennungseinrichtung ist

eine Linienverdünnung vorgesehen, welche die dicken Elemente der Fingerabdrucklinien von den zweidimensionalen Fingerabdruckdaten trennt, die von einer CCD-Kamera an die Merkmalerkennungseinrichtung übertragen worden sind. Ferner weist die Merkmalerkennungseinrichtung eine Mittelpositionserkennungseinrichtung auf, die den Mittelabschnitt der zweidimensionalen Fingerabdruckdaten bestimmt. Weiterhin ist eine Datenerkennungseinrichtung vorgesehen, die einen Fingerabdruckabschnitt innerhalb eines bestimmten Radius von der Mittelposition an erkennt, um ihn als Bestimmungsdaten darzustellen. Auf der Basis dieser Bestimmungsdaten erfolgt eine zweidimensionale Fourier-Transformation, in deren Ergebnis das zweidimensionale fouriertransformierte Bild als Spektrenmuster festgehalten wird.

Bei dieser Verfahrensweise wird zwar die erforderliche Speicherkapazität aufgrund der zweidimensionalen Fouriertransformation reduziert, nachteiligerweise ist aber immer noch ein Vergleich von Strukturen bzw. Strukturmustern der Daten, die von der eintretenden Person erfaßt werden, mit den Daten der registrierten Person erforderlich. Es gibt also eine Eindeutigkeit der gespeicherten Biometriedaten in Bezug auf die von der eintretenden Person neu eingelesenen Biometriedaten. Damit jedoch besteht nach wie vor die Möglichkeit einer Entschlüsselung der gespeicherten Fingerabdrücke und für den Vergleich bereitgehaltenen Daten; d. h. die Gefahr eines Mißbrauchs durch Unberechtigte ist nicht völlig ausgeschlossen.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der vorbeschriebenen Art so weiterzubilden, daß die Sicherheit noch weiter erhöht wird.

Die Aufgabe der Erfindung wird dadurch gelöst, daß in einem ersten Verfahrensschritt charakteristische biometrische Merkmale in Form hinreichend reproduzierbarer Merkmaldaten erfaßt werden, daß in einem weiteren Verfahrensschritt ein erster Datensatz aus Zufallsdaten generiert und als Steuerdatensatz auf einem Datenträger abgelegt wird, daß mindestens ein Teil der Merkmaldaten mit mindestens einem Teil des Steuerdatensatzes verknüpft und durch eine nicht umkehrbare Rechenoperation in einen zweiten Datensatz transformiert wird und daß der zweite Datensatz als Kriterium für die Erteilung der Zugang- und/oder die Ausübungsberechtigung und/oder als Kryptographieschlüssel verwendet wird.

Der wesentliche Unterschied zum Stand der Technik, der zugleich auch den bedeutenden Vorteil der Erfindung begründet, besteht darin, daß der zweite Datensatz zwar eindeutig ist in Bezug auf die Kombination des Steuerdatensatzes mit den Biometriedaten, die von der Eintritt begehrenden Person aufgenommenen werden, der zweite Datensatz jedoch nicht eindeutig ist in Bezug auf die eingelesenen Biometriedaten allein. Ein Bild- oder Strukturvergleich zur Identifizierung der Person bzw. der Biometriequelle (Finger, Gesichtszüge oder auch Stimme) ist nicht mehr möglich.

Der zweite Datensatz, der in der dargelegten Art und Weise erzeugt wird und als Zugangskriterium dienen soll, steht immer mit den eingelesenen Daten in Beziehung und wird bei jedem Eintritts begehren, auch wenn es sich dabei um dieselbe Person handelt, neu und abweichend generiert. Das aber heißt zugleich, daß keine Vorhersage zum Inhalt von weiteren erzeugten zweiten Datensätzen möglich ist, selbst wenn dieselben Biometriedaten zugrundegelegt werden. Damit ist gewährleistet, daß von unberechtigter Seite weder ein Rückschluß auf die Biometriedaten noch eine Vorschau auf die Datensätze möglich ist, die als Eintrittsbegehren generiert werden.

Sinnbildlich bedeutet das, daß als Zugangsvoraussetzung nicht wie bisher schlechthin ein Schlüssel für ein vorhande-

nes Schloß notwendig, sondern für jeden neuen Zugang ein neues, unvorhersehbares Schloß zu überwinden und dazu ein unbekannter Schlüssel erforderlich ist. Wird nun der zweite Datensatz gemeinsam mit dem Namen des Nutzers als Kriterium oder Paßwort einer Prüfung zugrunde gelegt, wird eine Zugangs- und/oder Ausübungsberechtigung nur den Personen zu erteilen, welche die entsprechende Identitätsvoraussetzung erfüllen.

Der Vorteil besteht weiterhin darin, daß ein extrem hohes Maß an Sicherheit gegeben ist, ohne daß der Benutzer bzw. derjenige, der Zutritt begehrt, eine Identifikationskarte oder einen ähnlichen Gegenstand, auf dem Daten gespeichert sind, mit sich führen muß. Die zu speichernden Daten sind im Vergleich zu bisher bekannten Verfahren so weit reduziert, daß nur noch eine wesentlich verringerte Speicherkapazität erforderlich ist. Außerdem ist es nicht mehr notwendig, die Einrichtung zum Einlesen der Merkmale beispielsweise mit einer Mittenpositionserkennung auszustatten oder eine Bildauswahleinheit im Hinblick auf einen Fingerabdruckabschnitt innerhalb eines bestimmten Radius von der Mittenposition vorzusehen. Die Anordnungen zur Ausübung des erfindungsgemäßen Verfahrens sind deshalb mit geringerem Aufwand herstellbar und haben aufgrund der unkomplizierteren Bauweise zugleich eine höhere Funktionssicherheit als die im Stand der Technik bekannten Anordnungen.

Eine sehr bevorzugte Weiterbildung der Erfindung besteht darin, daß die Rechenoperation zur Transformation der Daten nach einer cryptographischen HASH-Funktion erfolgt. Damit ist die Unumkehrbarkeit der Transformation mit hoher Sicherheit gewährleistet. Mit der Hash-Funktion wird eine variable Größe, zum Beispiel einen beliebigen Wertevorrat, in einen festen String überführt. Die Rechenoperation ist für beliebige Werte leicht auszuführen, jedoch nicht umkehrbar. Aus Eingangsgrößen beliebiger Länge werden Ausgangsgrößen fester Länge, die knapp aber präzise die ursprüngliche Information wiedergibt.

In einer vorteilhaften Ausgestaltung der Erfindung ist vorgesehen, daß zur Erzielung hinreichend reproduzierbarer Merkmaldaten die charakteristischen biometrischen Merkmale mehrfach erfaßt werden und nach jeder Datenerfassung jeweils eine Merkmalextraktion vorgenommen wird. Das hat den Vorteil, das die spätere Identifizierung mit höherer Sicherheit möglich ist. Die Merkmalextraktion kann dabei durch mehrfach ablaufende Bilderkennung und "Minutien-Detektion" analog zur kriminaltechnischen Bearbeitung vorgenommen werden.

In einer weiteren Ausgestaltung der Erfindung ist vorgesehen, daß nach jeder Merkmalextraktion eine Verifikation zur vorher erfolgten Datenerfassung vorgenommen wird. Durch den mehrfachen Durchlauf in Verbindung mit einer Verifikation kann mit erhöhter Sicherheit die spätere Speicherung entschlüsselbarer Daten ausgeschlossen werden.

Das erfindungsgemäße Verfahren kann in der Weise ausgeführt werden, daß die Generierung des Steuerdatensatzes (y) auf der Grundlage einer opto-elektronischen Aufnahme eines Fingerabdruckes vom Nutzer erfolgt, daß die gewonnenen Bilddaten in ein Datenverarbeitungssystem übernommen werden, daß anhand der Minutien des betreffenden Fingers entsprechend der vorgenannten Ansprüche Daten m gewonnen und nach der HASH-Funktion H(m) = f{y} in den Steuerdatensatz transformiert werden und dieser unkodiert unter dem Namen des Nutzers in einer Nutzerdatenbank auf dem Datenträger abgelegt wird.

Ein weiterer bedeutender Vorteil des vorgeschlagenen Verfahrens besteht darin, daß der Steuerdatensatz uncodiert ohne Gefahr einer unberechtigten Entschlüsselung auf dem Datenträger abgelegt werden kann.

Die Generierung des zweiten Datensatzes kann in der Weise erfolgen, daß durch Eingabe des Nutzernamens über eine Tastatur das Vorhandensein eines zugeordneten Steuerdatensatzes (y) auf dem Datenträger geprüft und gegebenenfalls aufgerufen wird, daß die optoelektronische Aufnahme des Fingerabdruckes des Nutzers erfolgt und daraus entsprechend der vorgenannten Ansprüche hinreichend reproduzierbare Merkmaldaten (x) gewonnen werden, daß die Daten (x) mit dem Steuerdatensatz (y) verknüpft und nach der HASH-Funktion H(z) = f{x,y} in einen zweiten Datensatz transformiert werden, der als "privater" Datensatz (z) als Kriterium für die Erteilung der Zugang- und/oder die Ausübungsberechtigung dient und/oder als Kryptographieschlüssel verwendet werden kann.

Das erfindungsgemäße Verfahren läßt sich zwar sehr gut anhand der biometrischen Daten eines Fingers anwenden, kann aber auch anderweitig, z. B. auf Grundlage der Gesichtsform oder auf Grundlage der Stimme, genutzt werden. In den ersten beiden genannten Fällen wird die Aufnahme der charakteristischen biometrischen Daten durch Erfassung elektronischer Bildinformationen vorgenommen, beim Zugrundlegen der Stimme dagegen werden die zu speichernden Daten anhand eines elektronischen Klangbildes erzeugt.

Die Erfindung bezieht sich weiterhin auf eine Anordnung zur Durchführung des Verfahrens, mit einem opto-elektronischen Bildwandler, einer Bilddatenverarbeitungseinheit und einer Datenausgabeeinheit, bei der zwischen der Bilddatenverarbeitungseinheit und der Datenausgabeeinheit eine Rechenschaltung zur nichtumkehrbaren Transformation der erfaßten Daten nach der HASH-Funktion H(m) = f{y} vorgesehen ist.

In einer weiteren Anordnung, die zur Generierung des zweiten Datensatzes genutzt werden kann und die über einen opto-elektronischen Bildwandler, eine Bilddatenverarbeitungseinheit, einen Datenträger, und eine Datenausgabeeinheit verfügt, ist im Signalweg zwischen der Bilddatenverarbeitungseinheit, dem Datenträger und der Datenausgabeeinheit eine Rechenschaltung zur Verknüpfung des Steuerdatensatzes (y) mit den Merkmaldaten (x) und zur Transformation nach der HASH-Funktion H(z) = f{x,y} in einen zweiten Datensatz vorgesehen.

Mit diesen vorgeschlagenen Anordnungen ist es vorteilhaft möglich, die weiter oben beschriebenen Verfahrensmerkmale funktionssicher auszuführen.

Die Erfindung soll nachfolgend an einem Ausführungsbeispiel näher erläutert werden. Soll ein neuer Nutzer beispielsweise in die Zugangsberechtigung zu einem nicht öffentlichen Datensystem einbezogen werden, so wird zunächst sein Name in die Nutzerdatenbank aufgenommen und ein Steuerdatensatz auf der Grundlage von Zufallsdaten erzeugt. Die Erzeugung des Steuerdatensatzes kann beispielhaft mit Hilfe des für die weiteren Verfahrensschritte vorhandenen hochauflösenden optischen Systems erfolgen, indem ein Fingerabdruck als elektronisches Bild aufgenommen, mittels Framegrabber in ein Datenverarbeitungssystem übertragen und die so vorliegenden Daten dann in der Rechenschaltung nach der HASH-Funktion H(m) = f{y} in den Steuerdatensatz transformiert und auf dem Datenträger zur weiteren Verwendung bereitgehalten wird.

Begehrt der Nutzer Zugang zu dem gesperrten Datensystem, wird er zunächst aufgefordert, seinen Namen über Tastatur einzugeben, woraufhin geprüft wird, ob der Nutzername bekannt ist; bei positivem Ergebnis wird der Steuerdatensatz aktiviert.

Jetzt wird der Nutzer aufgefordert, einen entsprechenden Finger auf den Fingerprint-Scanner zu legen und die Biometriedaten werden neu erfaßt, erneut ein elektronisches Bild erzeugt und dieses wiederum in das Datenverarbeitungssy-

stem eingelesen. Analog zur Minutien-Detektion der kriminaltechnischen Bearbeitung wird nun im Datenverarbeitungssystem eine Merkmalsextraktion vorgenommen. Das Einlesen der biometrischen Merkmale des Fingerabdruckes mit nachfolgender Merkmalsextraktion wird n-mal wiederholt.

Die eingelesenen Merkmaldaten und der Steuerdatensatz werden der Rechenschaltung nach der HASH-Funktion H(z) = f{x,y} zugeführt, dort miteinander verknüpft und in einen zweiten, einen sozusagen "privaten" Datensatz transformiert. Damit steht ein Datensatz zur Verfügung, der mit der vorbeschriebenen Sicherheit als Kriterium für die Erteilung der Zugangsberechtigung, einer Ausübungsberechtigung, als Kryptographieschlüssel oder auch anderweitig verwendet werden kann.

Werden beispielsweise sowohl der Nutzername als auch der "private" Datensatz, der die Funktion eines Paßwortes übernimmt, zur Prüfung an ein Kontrollsystem übergeben und ergibt die Kontrolle ein positives Ergebnis, wird der Zugang zum Datensystem für den Nutzer geöffnet.

Patentansprüche

1. Verfahren zur Identitätsprüfung als Voraussetzung für die Erteilung einer Zugangs- und/oder Ausübungsberechtigung, bei dem mit Hilfe eines Datenerfassungs- und Datenverarbeitungssystems mindestens ein Datensatz auf der Grundlage biometrischer Merkmale erzeugt wird und bei dem der Identitätsnachweis anhand der zugrundeliegenden biometrischen Merkmale erfolgt **dadurch gekennzeichnet,**
   - daß in einem ersten Verfahrensschritt charakteristische biometrische Merkmale in Form hinreichend reproduzierbarer Merkmaldaten erfaßt werden,
   - daß in einem weiteren Verfahrensschritt ein erster Datensatz aus Zufallsdaten generiert und als Steuerdatensatz auf einem Datenträger abgelegt wird,
   - daß mindestens ein Teil der Merkmaldaten mit mindestens einem Teil des Steuerdatensatzes verknüpft und durch eine nicht umkehrbare Rechenoperation in einen zweiten Datensatz transformiert wird und
   - daß der zweite Datensatz als Kriterium für die Erteilung der Zugangs- und/oder die Ausübungsberechtigung und/oder als Kryptographieschlüssel verwendet wird.

2. Verfahren zur Identitätsprüfung nach Anspruch 1, dadurch gekennzeichnet, daß die Rechenoperation zur Transformation der Daten nach einer kryptographischen HASH-Funktion erfolgt.

3. Verfahren zur Identitätsprüfung nach Anspruch 1, dadurch gekennzeichnet, daß zur Erzielung hinreichend reproduzierbarer Merkmaldaten die charakteristischen biometrischen Merkmale mehrfach erfaßt werden und nach jeder Datenerfassung jeweils eine Merkmalextraktion vorgenommen wird.

4. Verfahren zur Identitätsprüfung nach Anspruch 3, dadurch gekennzeichnet daß nach jeder Merkmalextraktion eine Verifikation zur vorhergehenden Datenerfassung vorgenommen wird.

5. Verfahren zur Identitätsprüfung nach einem der vorgenannten Ansprüche, dadurch gekennzeichnet, daß die Generierung des Steuerdatensatzes (y) auf der Grundlage einer opto-elektronischen Aufnahme eines Fingerabdruckes vom Nutzer erfolgt, daß die gewonnenen Bilddaten in ein Datenverarbeitungssystem übernommen werden, daß anhand der Minutien des betreffenden Fingers entsprechend der vorgenannten Ansprüche Daten in gewonnen und nach der HASH-Funktion H(m) = f{y} in den Steuerdatensatz transformiert werden und dieser unkodiert unter dem Namen des Nutzers in einer Nutzerdatenbank auf dem Datenträger abgelegt wird.

6. Verfahren zur Identitätsprüfung nach einem der vorgenannten Ansprüche, dadurch gekennzeichnet, daß zur Generierung des zweiten Datensatzes durch Eingabe des Nutzernamens über eine Tastatur das Vorhandensein eines zugeordneten Steuerdatensatzes (y) auf dem Datenträger geprüft und gegebenenfalls aufgerufen wird, daß die opto-elektronische Aufnahme des Fingerabdruckes des Nutzers erfolgt und daraus entsprechend der vorgenannten Ansprüche hinreichend reproduzierbare Merkinaldaten (x) gewonnen werden, daß die Daten (x) mit dem Steuerdatensatz (y) verknüpft und nach der HASH-Funktion H(z) = f{x,y} in einen zweiten Datensatz transformiert werden, der als "privater Datensatz (z) als Kriterium für die Erteilung der Zugangs- und/oder die Ausübungsberechtigung dient und/oder als Kryptographieschlüssel verwendet wird.

7. Anordnung zur Durchführung des Verfahrens nach den Ansprüchen 1 bis 6 mit einem opto-elektronischen Bildwandler, einer Bilddatenverarbeitungseinheit und einer Datenausgabeeinheit, dadurch gekennzeichnet, daß zwischen der Bilddatenverarbeitungseinheit und der Datenausgabeeinheit eine Rechenschaltung zur nichtumkehrbaren Transformation der erfaßten Daten nach der HASH-Funktion H(m) = f{y} vorgesehen ist.

8. Anordnung zur Durchführung des Verfahrens nach den Ansprüchen 1 bis 6, mit einem opto-elektronischen Bildwandler, einer Bilddatenverarbeitungseinheit, einem Datenträger, und einer Datenausgabeeinheit, dadurch gekennzeichnet, daß im Signalweg zwischen der Bilddatenverarbeitungseinheit, dem Datenträger und der Datenausgabeeinheit eine Rechenschaltung zur Verknüpfung des Steuerdatensatzes (y) mit den Merkmaldaten (x) und zur Transformation nach der HASH-Funktion H(z) = f{x,y} in einen zweiten Datensatz vorgesehen ist.